

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Applicants: Ricky F. COMBEST

Serial No.: 09/539,662

Group Art Unit: 2141

Filed: March 30, 2000

Examiner: Kristie D. Shingles

Att. Docket No.: T1142/20078

Confirmation No.: 8540

For: DYNAMIC VIRTUAL NETWORK AND METHOD

APPELLANTS' BRIEF

Mail Stop Appeal Brief-Patents
Commissioner for Patents
Board of Patent Appeals & Interferences
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This brief is being timely filed, under the provisions of 37 CFR §41.37. The required fee for a large entity set forth in 37 CFR §1.17(c) for the filing of this brief was previously paid with the Brief on Appeal filed in this application on December 14, 2006.

I. REAL PARTY IN INTEREST

T.C. License, Ltd., 8158 Adams Drive, Hummelstown, PA 17036 is the real party in interest regarding the above-identified application. T.C. License, Ltd. is owned by Roper Industries, Inc.

II. RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences known to the appellant, or the appellant's legal representatives, that will directly affect or be directly affected by, or have a bearing on, the Board of Patent Appeals and Interferences' decision in the pending appeal.

III. STATUS OF CLAIMS

Claims 1-7, 28-47 and 51 are pending in this application. These claims were rejected in a Final Rejection dated June 13, 2008. Claims 8-27 and 48-50 have been withdrawn from consideration.

Rejection of Claims 1-7, 28-47 and 51 is being appealed, and a copy of these claims is included in the Claims Appendix accompanying this brief.

IV. STATUS OF AMENDMENTS

No amendments have been filed subsequent to the Reply dated March 6, 2008.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The invention defined by Claim 1 and the claims dependent therefrom is directed to a dynamic virtual network on which participating members can establish partnerships, communicate, and share information, the network comprising: a network authority including a computer programmed for network administration (Fig. 3, network authority 302; page 9, lines 3-4 and 16-32); at least a first network member and a second network member, each member including a computer comprising means for communicating over a global network (Fig. 3, businesses 304; page 9, lines 6-7); at least a first network access device and a second network access device, wherein the first access device is accessible by the first network member and the second access device is accessible by the second network member, each of the first network access device and the second network access device storing information about the corresponding one of the first network member and the second network member such that the information is searchable by the other one of the first network member and the second network member (Fig. 3,

business network access appliances 303; page 9, lines 8-10; page 10, line 28, through page 12, line 5); and for each network access device and the network authority, an interface facilitating connection to a global network (Fig. 3, communication links 209; page 9, line 5).

The invention defined by claim 28 and the claims dependent therefrom is directed to a method for forming a partnership between two dynamic virtual network members connected by a network, the method comprising: selecting a partnership criterion by the first network member (Fig. 6, step 612; page 23, line 17); broadcasting the partnership criterion by the first network member to other network members (Fig. 6, step 622, page 23, lines 17-19); receiving by a second network member the partnership criterion; the second network member responding to the first network member (Fig. 6; steps 632, 634, and 636; page 23, lines 21-29); and establishing a partnership relationship between the first network member and second network member (Fig. 6, steps 614 and 624; page 23, line 31, through page 24, line 2).

The invention defined by claim 36 and the claims dependent therefrom is directed to a method for conducting a transaction between network members over the dynamic virtual network, the method comprising: transmitting and contemporaneously archiving information from a first network member to a second network member (Fig. 8, steps 811, 821, 822, 831, and 832; page 26, lines 16-33); and receiving and contemporaneously archiving the transmitted information by the second network member (Fig. 8, steps 841 and 842; page 27, lines 1-3).

Claim 37 depends from claim 36 and adds the further limitation that a priority network transmission is carried by a commercial global network service which provides business critical levels of service (Fig. 3, business exchange network 300 and communication links 209; page 8, lines 2-3; page 9, lines 2-5).

Claim 45 depends from claim 44, which depends from claim 36, and relative to claim 36, adds the further limitations that transmitting and contemporaneously archiving includes encrypting the information and that encrypting the transmitted information includes exchanging public keys between the first and second network members (exchange of keys, page 26, lines 7-9).

Claim 46 depends from claim 36 and adds the further limitation that receiving and contemporaneously archiving transmitted information includes digitally signing a document by the second network member (application of personal digital certificate/signature and logging of the transaction in permanent storage, page 27, lines 10-17).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. The rejection of claims 1-3 and 7 under 35 U.S.C. § 102(e) over Godefroid et al. (U.S. Patent No. 6,697,840). Claim 4 depends from Claim 1 and stands rejected over Godefroid in view of Schneider et al. (U.S. Patent No. 6,105,027). Claims 5 and 6 depend from Claim 1 and stands rejected over Godefroid in view of Kleinpeter III et al. (U.S. Patent No. 6,907,463). Claims 1-7 are argued as a group and stand or fall together.

2. The rejection of claims 28, 27-35 and 51 under 35 U.S.C. § 103(a) over Kleinpeter III view of Schneider. Claim 28 and 27-35 and 51 (all of which depend from Claim 28) are argued as a group. Claims 28-35 and 51 stand or fall together.

3. The rejection of claims 36, and 38-44 under 35 U.S.C. § 103(a) over Kleinpeter III view of Schneider. The rejections of claim 36, and 38-44 (all of which depend from Claim 36, which is substantially different than Claim 28) are argued as a group. Claims 36 and 38-44

stand or fall together.

4. The rejection of claims 37 and 46 under 35 U.S.C. § 103(a) over Godefroid in view of Kleinpeter III. Claims 37 and 46 are argued as a group and stand or fall together.

5. The rejection of Claim 45 under § 103(a) over Godefroid in view of Schneider.

VII. ARGUMENT

1. Rejection of Claims 1-3 and 7 under §102(e) over Godefroid.

The Examiner clearly erred in rejecting the subject claims as anticipated by Godefroid under 35 U.S.C. §102(e). Godefroid does not disclose a key element of Claim 1, namely that each of a first network access device and a second network access device store information about the corresponding one of a first network member and a second network member such that the information is searchable by the other one of the first network member and the second network member.

Godefroid is directed to a collaborative infrastructure implementing rules for “presence awareness” among a number of users. (col. 6, lines 50-67). The system has a plurality of user interfaces each connected to a separate controller. The controllers are connected to each other and to a server (“PA Server”) via a “collaboration bus.” The PA server hosts a “PA database that stores awareness information such as users’ private data, user activities, and awareness preference settings.” (col. 7, lines 2-5).

Claim 1 of the application under exam states

A dynamic virtual network on which participating members can establish partnerships, communicate, and share information, the network comprising:

a network authority including a computer programmed for network administration;

at least a first network member and a second network member, each member including a computer comprising means for communicating over a global network:

at least a first network access device and a second network access device, wherein the first access device is accessible by the first network member and the second access device is accessible by the second network member, each of the first network access device and the second network access device storing information about the corresponding one of the first network member and the second network member such that the information is searchable by the other one of the first network member and the second network member; and

for each network access device and the network authority, an interface facilitating connection to a global network.

The Examiner alleges that Godefrid discloses “at least a first network access device and a second network access device, wherein the first access device is accessible by the first network member and the second access device is accessible by the second network member, each of the first network access device and the second network access device storing information about the corresponding one of the first network member and the second network member such that the information is searchable by the other one of the first network member and the second network member.” (Final Rejection mailed June 13, 2008 at p.3).

Godefrid does not disclose network access devices that store information that is searchable by other network access devices. In Godefrid, the information that is searchable is stored on a central “PA database” not the individual network devices. (col. 7, lines 3-5, 45-49).

“In the PA system, the PA Database and PA server form a centralized database which stores all awareness information, such as all users’ private data, users’ activities and awareness preferences settings.” Nowhere does Godefroid disclose or suggest that individual network devices have direct access to other individual network devices such that the information stored by one network member is searchable by another other network member. The whole point of Godefroid is to protect the privacy of individual network devices by having a centralized database—the PA Database—that stores only awareness information. (col. 7, lines 45-61). Allowing individual network devices to search information stored on other network devices as stated in Claim 1, is not compatible with Godefroid which seeks to isolate individual devises for privacy and security reasons.

For these reasons, Claim 1 is believed to be allowable. Claims 2-7 depend from Claim 1 and are allowable for at least the reasons explained above with respect to Claim 1.

2. Rejection of claims 28, 27-25 and 51 under 35 U.S.C. § 103(a) over Kleinpeter III view of Schneider.

Before the specifics of the claims are discussed relative to the applied prior art, the Appellant wishes to note the following principles of law, which the Appellant wishes to apply to the discussion of each particular claim rejection based on 35 U.S.C. §103(a)

Under Section 103(a), “a patent may not be obtained. . . if the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.” 35 U.S.C. §103(a). Graham v. John Deere Co. of Kansas City, 383 U. S. 1 (1966), sets out the objective analysis for applying Section 103:

(T)he scope and content of the prior art are . . . determined; differences between the prior art and the claims at issue are . . . ascertained; and the level of ordinary skill in the pertinent art resolved. Against this background the obviousness or nonobviousness of the subject matter is determined. Such secondary considerations as commercial success, long felt but unsolved needs, failure of others, etc., might be utilized to give light to the circumstances surrounding the origin of the subject matter sought to be patented.

383 U.S. at 17-18. With regard to a rejection under 35 U.S.C. § 103(a) over a combination of references, the mere fact that every element of the claimed invention can be found in the prior art does not suffice to show that the combination would have been obvious. In re Rouffet, F.3d 1350, 1357, 47 U.S.P.Q.2d 1453, 1457 (Fed. Cir. 1998). Such a ground of rejection would constitute impermissible hindsight. Id. When combining known elements from multiple references to demonstrate obviousness, an examiner must identify “some motivation or suggestion to combine the prior art teachings in the prior art, the nature of the problem, or the knowledge of a person having ordinary skill in the art.” KSR Intern. Co. v. Teleflex Inc., 127 S.Ct. 1727, 1730.

In addition, the examiner is not at liberty to pick and choose which teachings to apply from each reference. Instead, the examiner is legally bound to consider “disclosures in the references that diverge from and teach away from the invention at hand.” W. L. Gore & Associates, Inc., v. Garlock, Inc., 721 F.2d 1540, 1550, 220 U.S.P.Q. 303, 311 (Fed. Cir. 1983).

With these principles in mind, the Examiner clearly erred in rejecting Claim 28, and claims 27-35 and 51, which depend from Claim 28, under 35 U.S.C. § 103(a) over Kleinpeter III view of Schneider. Kleinpeter III is directed to a means to exchange files between users in a

network environment by use of a software agent on each user's computer. An agent server directs the software agents to establish direct connections between user systems in response to file requests. (Abstract).

Claim 28 states:

A method for forming a partnership between two dynamic virtual network members connected by a network, the method comprising:
selecting a partnership criterion by the first network member;
broadcasting the partnership criterion by the first network member to other network members;
receiving by a second network member the partnership criterion;
the second network member responding to the first network member; and
establishing a partnership relationship between the first network member and second network member.

The Examiner admits that Kleinpeter III does not teach virtual network members. (Office Action p. 5.) To overcome this deficiency, the Examiner cites Schneider. Schneider is directed to an access filter for a virtual private network where access filters control access to information that is stored in servers in the network by users at clients in the network. Each access filter uses a local copy of an access control data base to determine whether an access request has been made by a user. Changes to the local copies are propagated to all of the local copies. (Abstract). There would have been no motivation to combine Schneider with Kleinpeter III because the updating of local copies of the access control data base in Schneider makes the agent server in Kleinpeter III unnecessary. Combining the two would produce redundant features that make no logical or practical sense.

For the reasons set forth above, the Appellant respectfully submits that the rejection is

unfounded and should be reversed.

3. Rejection of claims 36, and 38-44 under 35 U.S.C. § 103(a) over Kleinpeter III view of Schneider.

The Examiner argued that Claim 36 is “substantially similar to claim 28” and rejected it on the same basis as the rejection of Claim 28.

Claim 36 states:

A method for conducting a transaction between network members over the dynamic virtual network, the method comprising:
transmitting and contemporaneously archiving information from a first network member to a second network member; and
receiving and contemporaneously archiving the transmitted information by the second network member.

The Appellant disagrees that Claim 36 is substantially similar to Claim 28 and asserts that Kleinpeter III and Schneider either alone or in combination do not disclose all of the elements of Claim 36. To the extent the Examiner relies on the rejection of Claim 28, the Appellant restates the reasons set forth above with respect to that claim as to why the rejection is improper and respectfully submits that the rejection of Claim 36 and claims 38-44 that depend from Claim 36, is unfounded and should be reversed.

4. The rejection of claims 37 and 46 under 35 U.S.C. § 103(a) over Godefroid in view of Kleinpeter III.

Claim 36, from which claims 37 and 46 depend, states a method comprising “transmitting and contemporaneously archiving information from a first network member to a second network member; and receiving and contemporaneously archiving the transmitted information by the

second network member.” The Examiner has not pointed to any portion of Godefroid that discloses or suggests this. As explained above, in Godefroid, information about network members is stored in a central database, not other network members. Kleinpeter does not disclose or suggest the deficiencies in Godefroid. Additionally, the Appellant refers to the previous response to the Examiner’s rejection of Claim 36, from which Claim 45 depends.

While the Examiner has grouped the rejection of Claims 37 and 46 under a heading based on a §103(a) rejection based on Godefroid in view of Kleinpeter III, the Examiner argued that Claims 37 and 46 are substantially similar to Claims 2 and 3 respectively and rejected them on the same bases, i.e. on Godefroid alone. (Office Action p. 9). The Appellant disagrees that these claims are similar. To the extent, however, that the Examiner relies on the rejection of Claims 2 and 3, the Appellant incorporates the remarks stated above with respect to the rejection of Claim 1 based on Godefroid.

The Appellant restates the reasons set forth above as to why the rejection of Claim 36 is improper in as much Claims 37 and 46 depend from Claim 36. For these reasons, the Appellant respectfully submits that the rejection of Claims 37 and 46 is unfounded and should be reversed.

5. The rejection of Claim 45 under § 103(a) over Godefroid in view of Schneider.

Claim 45 depends from Claim 36, which states a method comprising “transmitting and contemporaneously archiving information from a first network member to a second network member; and receiving and contemporaneously archiving the transmitted information by the second network member.” Godefroid does not disclose or suggest this. As explained above, in

Godefroid, information about network members is stored in a central database, not other network members. The Examiner states that Claim 45 is substantially similar to Claim 4, however Claim 1, from which Claim 4 depends does not state “transmitting and contemporaneously archiving information from a first network member to a second network member.” The Examiner has not pointed to any portion of Godefroid that discloses or suggests this. Schneider does not disclose or suggest the deficiencies in Godefroid. The Appellant restates the reasons set forth above as to why the rejection of Claim 36 is improper inasmuch as Claim 45 depends from Claim 36. For these reasons, the Appellant respectfully submits that the rejection of Claim 45 is unfounded and should be reversed.

CONCLUSION

For the reasons set forth above, the Appellant respectfully submits that the present claims define subject matter that would not have been anticipated by or obvious over the combination of references proposed in the Final Rejection. Therefore, the Appellant respectfully urges that all grounds of rejection set forth in the Final Rejection be reversed.

For all of the reasons set forth above, the Appellant respectfully urges reversal of the rejection of claims 1-7, 28-47, and 51.

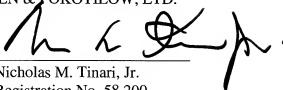
Respectfully submitted,

CAESAR, RIVISE, BERNSTEIN,
COHEN & POKOTILOW, LTD.

September 12, 2008

Please charge or credit our
Account No. 03-0075 as necessary
to effect entry and/or ensure
consideration of this submission.

By



Nicholas M. Tinari, Jr.
Registration No. 58,200
Customer No. 03000
(215) 567-2010
Attorneys for Appellant

CLAIMS APPENDIX

The following is a list of the claims involved in the appeal in their current form.

1. A dynamic virtual network on which participating members can establish partnerships, communicate, and share information, the network comprising:

a network authority including a computer programmed for network administration;

at least a first network member and a second network member, each member including a computer comprising means for communicating over a global network;

at least a first network access device and a second network access device, wherein the first access device is accessible by the first network member and the second access device is accessible by the second network member each of the first network access device and the second network access device storing information about the corresponding one of the first network member and the second network member such that the information is searchable by the other one of the first network member and the second network member; and

for each network access device and the network authority, an interface facilitating connection to a global network.

2. The network claimed in claim 1, wherein the global network interface provides priority network transmission by connection to a commercial global network system which provides business critical levels of service.

3. A dynamic virtual network claimed in claim 1, including means for communication between the first and second network access devices, and the network authority, which utilizes digital certificates.

4. A dynamic virtual network claims in claim 1, wherein at least the first and second network members include means for exchanging public keys.

5. A dynamic virtual network claimed in claim 1, wherein the network authority further includes a means for contemporaneously archiving a communication transmitted over the network.

6. A dynamic virtual network claimed in claim 1, wherein each network access device includes a means for contemporaneously archiving a communication transmitted through the device.

7. A dynamic virtual network claimed in claim 1, including means for enabling limited access to the member's information to other network members, while excluding non-members from access.

28. A method for forming a partnership between two dynamic virtual network members connected by a network, the method comprising:

selecting a partnership criterion by the first network member;

broadcasting the partnership criterion by the first network member to other network members;

receiving by a second network member the partnership criterion;

the second network member responding to the first network member; and

establishing a partnership relationship between the first network member and second network member.

29. A method for forming a partnership over the dynamic virtual network as claimed

in claim 28, wherein the network members are connected to the network via a network access device which denies network access to net non-members.

30. A method for forming a partnership over the dynamic virtual network as claimed in claim 28, wherein the establishment step grants the first network member access to private data via the second network member's access drive.

31. A method for forming a partnership over the dynamic virtual network as claimed in claim 28, wherein the establishment step grants the first network member access to private data on the second network member's shared storage area.

32. A method for forming a partnership over the dynamic virtual network as claimed in claim 28, wherein the establishment step includes transmittal by the first network member to the second network member of authorization to access private data on the first network member's network access device.

33. A method for forming a partnership over the dynamic virtual network as claimed in claim 28, wherein the establishment step includes transmittal by the first network member to the second network member of authorization to access private data on the first network member's share storage area.

34. A method for forming a partnership over the dynamic virtual network as claimed in claim 28, wherein the establishment step includes permitting access by the first network member partner to role information of the second network member partner.

35. A method for forming a partnership over the dynamic virtual network as claimed in claim 28, wherein the partnership establishment includes reciprocally permitting access by one network member partner to role information of the other network member partner.

36. A method for conducting a transaction between network members over the dynamic virtual network, the method comprising:

transmitting and contemporaneously archiving information from a first network member to a second network member; and

receiving and contemporaneously archiving the transmitted information by the second network member.

37. A method for conducting a transaction between network members over the dynamic virtual network as claimed in claim 36, wherein a priority network transmission is carried by a commercial global network service which provides business critical levels of service.

38. A method for conducting a transaction between network members over the dynamic virtual network as claimed in claim 36, further comprising the steps of

transmitting and contemporaneously archiving by the second network member a response to the first network member; and

receiving and contemporaneously archiving by the first network member the response received.

39. A method for conducting a transaction between network members over the dynamic virtual network as claimed in claim 36, wherein the transmitted information is contemporaneously archived by the network authority.

40. A method for conducting a transaction between network members over the dynamic virtual network as claimed in claim 36, wherein the archiving control element resides in the network access device.

41. A method for conducting a transaction between network members over the dynamic virtual network as claimed in claim 36, wherein transmitting and contemporaneously archiving information includes transmitting and contemporaneously archiving a document whose terms are unalterable.

42. A method for conducting a transaction between network members over the dynamic virtual network as claimed in claim 36, wherein receiving and contemporaneously archiving the transmitted-information includes sending a return receipt.

43. A method for conducting a transaction between network members over the dynamic virtual network as claimed in claim 36, further comprising establishing a partnership between the first and second network members before the transmitting and contemporaneous archiving step.

44. A method for conducting a transaction between network members over the dynamic virtual network as claimed in claim 36, wherein transmitting and contemporaneously archiving includes encrypting the information.

45. A method for conducting a transaction between network members over the dynamic virtual network as claimed in claim 44, wherein encrypting the transmitted information includes exchanging public keys between the first and second network members.

46. A method for conducting a transaction between network members over the dynamic virtual network as claimed in claim 36, wherein receiving and contemporaneously archiving transmitted information includes digitally signing a document by the second network member.

47. A method for conducting a transaction between network members over the

dynamic virtual network as claimed in claim 46, wherein receiving and contemporaneously archiving transmitted information further includes transmitting the signed document to the first network member.

51. The method of claim 28, wherein the partnership criterion is expressed as a search, and wherein the step of receiving comprises performing the search at the second network member.

EVIDENCE APPENDIX

(None)

RELATED PROCEEDINGS APPENDIX

(None)